Better Internet for Kids

Self-assessment tool on age assurance: Manual

May 2024

Self-assessment tool on age assurance: Manual

Written by:

Mohammed Raiz Shaffique LLM and Professor Simone van der Hof, Center for Law and Digital Technologies (eLaw), Leiden University, Leiden, The Netherlands.

The publication of this document has been coordinated by European Schoolnet on behalf of the European Commission in the framework of the EC's Better Internet for Kids (BIK) initiative, with funding provided by the Digital Europe Programme (DIGITAL).

Contents

Abbreviations

ACCS	Age Check Certification Scheme
AEPD	Spanish Data Protection Agency | Agencia Española de Protección de Datos (Spain)
Agcom	Communications Regulatory Authority | Autorità per le Garanzie nelle Comunicazioni (Italy)
Arcom	Regulatory Authority for Audiovisual and Digital Communication | Autorité de régulation de la communication audiovisuelle et numérique (France)
AVMSD	Audiovisual Media Services Directive
BIK+	Better Internet for Kids
BSI	British Standards Institution
CNM	Media Commission | Coimisiún na Meán (Ireland)
CNMC	National Markets and Competition Commission | Comisión Nacional de los Mercados y la Competencia (Spain)
CRIA	Child Rights Impact Assessment
DPC	Data Protection Commission (Ireland)
DPIA	Data Protection Impact Assessment
DSA	Digital Services Act
EDPB	European Data Protection Board
ERGA	European Regulators Group for Audiovisual Media Services

ETSI	European Telecommunications Standards Institute
EU	European Union
EUDI	EU digital identity
GCHQ	Government Communications Headquarters (UK)
GDPR	General Data Protection Regulation
ICO	Information Commissioner's Office (UK)
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
KJM	Commission for the Protection of Minors in the Media | Kommission für Jugendmedienschutz (Germany)
NIST	National Institute of Standards and Technology (United States)
OECD	Organisation for Economic Co-operation and Development
Ofcom	Office of Communications (UK)
UK	United Kingdom
UN CRC	United Nations Convention on the Rights of the Child 1989 (including its optional protocols)
UNICEF	United Nations Children's Fund

1. Introduction

1.1 Background

Age assurance has been considered by policymakers, civil society groups and other organisations as one of the solutions for the protection of children online, given the various risks faced by children online.[1] The European Commission's BIK+ strategy, which was published on 11 May 2022,[2] safeguards the protection of children against online risks, while promoting children's well-being by creating safe and age-appropriate digital environments, and by respecting children's rights and their best interests in general. One of the actions under the BIK+ strategy is to draft a request for a European standard on age verification online.[3] In the context of the Digital Services Act (DSA), the European Commission has also recently formed a task force with the member states, the European Data Protection Board (EDPB) and the European Regulators Group for Audiovisual Media Services (ERGA), to promote cooperation, identify best practices and develop an EU-wide approach to age verification, in the framework of the EU digital identity (EUDI) wallet.[4]

[1] OECD. (2021). *Children in the digital environment: Revised typology of risks*. https://www.oecd-ilibrary.org/science-and-technology/children-in-the-digital-environment_9b8f222e-en; Livingstone, S., & Stoilova, M. (2021). The 4Cs: Classifying online risk to children. *Leibniz-Institut Für Medienforschung | Hans-Bredow-Institut (HBI)*. https://doi.org/10.21241/ssoar.71817.

[2] European Commission. (11.05.2022). *A Digital Decade for children and youth: the new European strategy for a better internet for kids (BIK+)*. https://digital-strategy.ec.europa.eu/en/library/digital-decade-children-and-youth-new-european-strategy-better-internet-kids-bik.

[3] European Commission. (11.05.2022). *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS. A Digital Decade for children and youth: the new European strategy for a better internet for kids (BIK+)*. COM(2022) 212 final. Pg. 11. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022DC0212.

[4] European Commission. (30.01.2024). *Digital Services Act: Task Force on Age Verification*. https://digital-strategy.ec.europa.eu/en/news/digital-services-act-task-force-age-verification-0; European Commission. (20.03.2024). *Second Meeting of the Task Force on Age Verification*. https://digital-strategy.ec.europa.eu/en/news/second-meeting-task-force-age-verification.

Several studies[5] have been undertaken regarding age assurance, and there are also standards[6] being developed with respect to the same. Guidance on implementing age assurance in specific contexts, such as the protection of children from age-inappropriate content, is also present in several jurisdictions.[7] However, age assurance is a complex topic and its optimal practical implementation differs on a case-by-case basis, depending on the given situations.

For a comprehensive analysis of the various dimensions of age assurance, please see the report titled 'Research report: Mapping age

[5] E.g., 5Rights Foundation. (Oct 2021). *But how do they know it is a child?. Age Assurance in the Digital World*; GCHQ. (Nov 2020). VoCO (Verification of Children Online). Phase 2 Report. https://www.gov.uk/government/publications/voco-verification-of-children-online-phase-2-report; UNICEF. (Apr 2021). Digital Age Assurance Tools and Children's Rights Online across the Globe: A Discussion Paper. https://c-fam.org/wp-content/uploads/Digital-Age-Assurance-Tools-and-Childrens-Rights-Online-across-the-Globe.pdf.

[6] IEEE. (Feb 2024). IEEE Approved Draft Standard for Online Age Verification. *IEEE P2089.1/D2.1*. The draft standard that was being developed by the ISO, i.e. ISO/IEC 27566, is now deleted and is proposed to be replaced by two new draft standards, namely ISO/IEC WD 27566-1 and ISO/IEC WD 27566-2. *See* ISO. (n.d.). ~~*ISO/IEC WD 27566. Information security, cybersecurity and privacy protection. Age assurance systems Framework*~~. https://www.iso.org/standard/80399.html; ISO. (n.d.). *ISO/IEC WD 27566-1. Information security, cybersecurity and privacy protection. Age assurance systems Framework. Part 1: Framework*. https://www.iso.org/standard/88143.html; and ISO. (n.d.). *ISO/IEC WD 27566-2: Age assurance systems. Part 2: Benchmarks for benchmarking analysis*. https://www.iso.org/standard/88147.html respectively.

[7] AEPD. (Dec 2023). *Decálogo de principios. Verificación de edad y protección de personas menores de edad ante contenidos inadecuados.* https://www.aepd.es/guias/decalogo-principios-verificacion-edad-proteccion-menores.pdf; CNMC. (n.d.). *PUBLIC CONSULTATION ON THE CRITERIA FOR ENSURING THE APPROPRIATENESS OF AGE VERIFICATION SYSTEMS ON VIDEO-SHARING PLATFORM SERVICES FOR CONTENT THAT IS HARMFUL FOR MINORS*. INF/DTSA/329/23. https://www.cnmc.es/sites/default/files/editor_contenidos/Audiovisual/1_1_INF_DTSA_329_23_Public%20consultation%20age%20verification%20CNMC%20Spain_eng.pdf; KJM. (12.05.2022). *Kriterien zur Bewertung von Konzepten für Altersverifikationssysteme als Elemente zur Sicherstellung geschlossener Benutzergruppen in Telemedien nach § 4 Abs. 2 S. 2 JMStV*. https://www.kjm-online.de/fileadmin/user_upload/KJM/Themen/Technischer_Jugendmedienschutz/AVS-Raster_gueltig_seit_12.05.2022-ENG.pdf; Ofcom. (05.12.2023). *Guidance on age assurance and other Part 5 duties for service providers publishing pornographic content on online services*. https://www.ofcom.org.uk/__data/assets/pdf_file/0018/272601/guidance-part-5-annexe-2.pdf; Arcom. (April 2024). *Consultation publique sur le projet de référentiel déterminant les exigences techniques minimales applicables aux systèmes de vérification de l'âge mis en place pour l'accès à certains services de communication au public en ligne et aux plateformes de partage de vidéos qui mettent à disposition du public des contenus pornographiques*. https://www.arcom.fr/sites/default/files/2024-04/Arcom-Consultation-publique-projet-referentiel-determinant-exigences-techniques-minimales-applicables-aux-systemes-verification-age-acces-contenus-pornographiques-en-ligne.pdf; CNM. (08.12.2023). *Consultation Document: Online Safety*. https://www.cnam.ie/wp-content/uploads/2023/12/Draft_Online_Safety_Code_Consultation_Document_Final.pdf; Agcom. (06.03.2024). *CONSULTAZIONE PUBBLICA DI CUI AL COMMA 4 DELLA DELIBERA N. 9/24/CONS PER L'APPROVAZIONE DI UN PROVVEDIMENTO CHE DISCIPLINA LE MODALITÀ TECNICHE E DI PROCESSO PER L'ACCERTAMENTO DELLA MAGGIORE ETÀ DEGLI UTENTI AI SENSI DELLA LEGGE 13 NOVEMBRE 2023, N. 159*. https://www.agcom.it/documents/10179/33556820/Allegato+25-3-2024+1711363896057/490138bb-c739-4f2f-81ac-21acc717767e?version=1.0.

assurance typologies and requirements'.[8] Published under the BIK+ initiative, it is used by the present self-assessment tool to elaborate further on various aspects related to age assurance that are discussed in this document.

Thus, the present self-assessment tool seeks to provide guidance to digital service providers on making decisions related to age assurance so that they can have a robust age assurance process in place.

This self-assessment tool should be viewed as guidance and not as a legal compliance mechanism, including as implying compliance under the Audiovisual Media Services Directive (AVMSD), the Digital Services Act (DSA), or the General Data Protection Regulation (GDPR). This self-assessment tool should be used in a context-specific manner regarding the particularities associated with a given digital service.

It is strongly advised that digital service providers complement this self-assessment tool along with other assessments, such as a Child Rights Impact Assessment (CRIA), Data Protection Impact Assessment (DPIA), and Fundamental Rights Impact Assessment (FRIA) for high-risk artificial intelligence (AI) systems, and with their own legal assessment of compliance with their various obligations in this context.

This self-assessment tool comprises two parts:

(i) an age assurance questionnaire (Questionnaire), and

(ii) an age assurance manual (Manual – this document).

The manual can be used by digital service providers to understand, in more detail, the relevant concepts related to age assurance and as guidance on how to navigate

[8] Shaffique, M.R. & van der Hof, S. (Feb 2024). Research report: Mapping age assurance typologies and requirements. European Commission. https://data.europa.eu/doi/10.2759/455338.

the questionnaire. The section numbers of the manual correspond to the section numbers of the questionnaire for ease of reference.

This manual is structured as follows: after the present background section (Section 1.1), a better understanding of the relevant terms for this self-assessment tool is provided (Section 1.2). Thereafter, Section 2 contains substantive guidance with respect to answering the questions in the questionnaire. It consists of introductory guidance on how to navigate that section, which is followed by explanations about the five steps to be taken concerning age assurance and cross-cutting considerations.

1.2 Relevant terminology

The following are the main terminologies that are relevant for the purpose of the present self-assessment tool:

Age assurance is the umbrella term for the methods that are used to determine the age or age range of an individual to varying levels of confidence or certainty.[9] The three primary categories of age assurance methods are **age estimation**, **age verification** and **self-declaration**.[10]

Age estimation consists of methods which establish that "a user is likely to be of a certain age, fall within an age range, or is over or under a certain age. Age estimation methods include [estimation based on facial features,][11] automated analysis of behavioural and environmental data, comparing the way a user interacts with a device with other users of the same age, and metrics derived from motion analysis or by testing their capacity or knowledge".[12]

[9] euCONSENT. (29.06.2021). *D5.1 Common Vocabulary*. Pg. 4. https://euCONSENT.eu/project-deliverables/.

[10] *Id*.

[11] Added by the authors.

[12] CEN and CENELEC. (Sep 2023). *Age appropriate digital services framework*. Pg. 10. https://www.cencenelec.eu/media/CEN-CENELEC/CWAs/ICT/cwa18016_2023.pdf.

Age verification is "a system that relies on hard (physical) identifiers and/or verified sources of identification that provide a high degree of certainty in determining the age of a user. It can establish the identity of a user but can also be used to establish [whether the user is over a certain minimum or under a certain maximum][13] age only".[14]

Self-declaration is a category of age assurance which consists of methods that rely on the individual to supply their age or confirm their age range without providing any evidence to prove such declaration.[15] Examples of self-declaration methods include declaring one's date of birth or declaring that one is above 18 years of age.

For a further elaboration of the difference (a) between age assurance and age verification, and (b) between age verification and age estimation, please see Section 2.1 of the report on Mapping age assurance typologies and requirements.

In addition to the above, it is vital to understand the meanings ascribed to the following terms in the present self-assessment tool:

The term **age assurance method** is used to denote the various types or categories of age assurance, such as hard identifiers (which is an age verification method), facial age estimation (which is an age estimation method), and so on (as further elaborated under Section 2, Step 3). Age assurance methods are thus sub-sets of age assurance, which fall under one

[13] Added by the authors.

[14] CEN, *supra* note 12 at 10.

[15] ICO. (15.01.2024). *Information Commissioner's opinion: Age Assurance for the Children's Code*. Pg. 9. https://ico.org.uk/about-the-ico/what-we-do/information-commissioners-opinions/age-assurance-for-the-children-s-code/.

of the three broad categories of age verification, age estimation and self-declaration.

The term **age assurance tool**[16] is a sub-set of an age assurance method and is used to denote the type of age assurance technology used. For instance, 'company XYZ' which provides facial age estimation services, is an age assurance tool falling under the age assurance method of facial age estimation.

The term **age assurance process**[17] denotes the entire process adopted by digital service providers to implement age assurance.[18] This process can involve a combination of age assurance methods and tools.

The term **level of assurance**[19] denotes the degree of confidence that can be placed in the user's age or age range being accurately determined by the age assurance process.[20]

For a further elaboration of other terms which are used in connection with age assurance (i.e., age-appropriate design, age gating, age ratings, age token, parental consent and parental control), please see Section 2.2 of the report on Mapping age assurance typologies and requirements.

[16] This term is also referred to as 'age assurance component' in certain literature. *See* ISO. (Nov 2021). *ISO Working Draft Age Assurance Systems Standard*. Pg. 5. https://euconsent.eu/download/iso-working-draft-age-assurance-systems-standard/.

[17] This term is also referred to as 'age assurance systems' in certain literature. *See Ibid* at 10.

[18] Ofcom, *supra* note 7 at 14.

[19] This term is also referred to as 'level of confidence' or 'level of age confidence' in certain literature. *See* IEEE, *supra* note 6 at 9; and GCHQ, *supra* note 5 at 18 respectively.

[20] ISO, *supra* note 16 at 13.

2. Guidance on the questionnaire

The present guidance on the questionnaire is to be navigated as follows:

Step 1: This step involves a preliminary setting of the stage phase (questions 1.1 and 1.2), whereby the nature of the digital service and its risks to online child safety are analysed. This preliminary assessment is then used to determine the likely requirement for age assurance (questions 1.3 to 1.5). This analysis of requirement for age assurance can help guide the decision of whether the remaining steps are relevant for the digital service provider.

Step 2: If it is determined that age assurance should be implemented as per Step 1, the level of assurance required of the age assurance process is to be ascertained in this step. While determining levels of assurance of age assurance processes is still an area under development, the present step provides some indicative guidance as to how this can be assessed.

Step 3: This step involves the actions to be undertaken to identify the age assurance tool(s) that can be utilised by the digital service provider, which could provide the required level of assurance. This involves an analysis of the availability of age assurance tool(s) (question 3.1), the various advantages and disadvantages associated with such tool(s) (question 3.2), and so on. This step culminates in a holistic analysis of the age assurance process to be implemented proportionately given the identified age assurance tool(s) (question 3.5).

Step 4: At this stage, important factors to be considered while implementing age assurance are assessed. This includes factors such as whether circumvention techniques are addressed (question 4.5), how transparency will be maintained concerning age assurance (question 4.9), and so on.

Step 5: This step is concerned with monitoring the performance of age assurance processes and undertaking a periodic review of them. Doing so can help the digital service provider analyse whether the previous steps' decisions need to be reconsidered.

Relevant cross-cutting considerations: This part discusses two cross-cutting aspects to be considered while implementing age assurance: first, hearing the views of children and other stakeholders, and second, ensuring legal compliance.

Digital service providers using this self-assessment tool must acknowledge that different parts or functionalities of their service(s) may have diverging age assurance requirements. Where the present self-assessment tool refers to a digital service, this also includes a reference to specific parts or functionalities of that digital service which may have such diverging age assurance requirements.

Finally, certain questions of this self-assessment tool contain reporting examples. These are kept brief in nature and are solely for illustration purposes. They should not be viewed as a suggestion or endorsement of any particular way of performing age assurance or maintaining records relating to age assurance.

Step 1 – Ascertaining the need for age assurance

The preliminary stage when it comes to age assurance involves an assessment of whether age assurance is to be implemented by the digital service provider. The preliminary questions 1.1 to 1.2 below help the digital service provider document and elaborate on the functioning of its digital service. This can, in turn, aid the digital service provider in ascertaining the requirement for age assurance and answering the subsequent questions in this self-assessment tool.

Q1.1 What is the nature of the digital service?

…

Describe the digital service provided to users. If it is a service that is planned to be provided, such a description has to be given based on estimation or forecasting. This description of the service can be crucial in informing the digital service provider of the next step of assessing the risks of the digital service. If such descriptions have already been made for assessments such as a Child Rights Impact Assessment (CRIA), Data Protection Impact Assessment (DPIA), and Fundamental Rights Impact Assessment (FRIA) for high-risk artificial intelligence (AI) systems, the same can be used and reproduced here. Needless to say, examining the facts to provide such a description should be done in compliance with the law, including data protection law and platform regulation.

Include *inter alia* explanations about aspects such as:

(i) What is the objective of the digital service?

Elaborate about what is intended to be achieved through the digital service. If the digital service is not in actual operation, mention the intended time for operation.

(ii) What is the technology used?

Specify as to what the underlying technology employed is and, for instance, whether advanced technologies such as AI or biometrics are used.

(iii) What is the nature, scope, context and purpose of the data that is processed?

Elaborate about the types of data that are processed (for example, personal data, anonymised data, metadata, and so on) and how such data is processed.

(iv) Which jurisdictions is the digital service made available in?

Identify aspects such as whether the service is provided worldwide or to users of specific countries, and similar. Factors such as who can use the services provided, who the service is marketed at, the language options that are provided, and so on, can help such an analysis.

(v) Who are the users?

Assess the type and number of existing and potential users of the digital service. Establish the age or age range of such users, particularly if the users are or may be children. This can be estimated by using various factors such as the nature of users in similar services, whether the design of the digital service or marketing of the digital service is intended to appeal to children, and other research or market evidence (for example, indicators such as higher user traffic after school hours or during school holidays)[21].

Reporting example: The digital service is an existing online fashion intermediary marketplace. The objective of the entity is to provide a digital service where various interested parties, such as consumers, designers, and retailers, can view, market, and sell fashion products. The digital service utilises algorithms for product recommendation and also has in place payment gateways for transactions to be processed. Various types of data, including user profiles, browsing history,

[21] ICO. (n.d.). 'Likely to be accessed' by children – FAQs, list of factors and case studies. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/likely-to-be-accessed-by-children/#threshold.

purchase behaviour, payment information, and communication logs are processed. The digital service is provided globally and can be accessed in multiple countries across the world. Various individuals and entities, such as consumers, designers, retailers, marketing experts, and so on use the digital service, and the monthly user numbers are estimated at around 200,000 to 250,000. The users of this digital service could include children and their parents, as products for children of all ages are made available on the marketplace.

Q1.2 What are the (potential) risks posed by the digital service to children, and what are the levels of these risks?

Type of risk and description	Probability of risk	Impact of risk	Risk assessment
(e.g., content risk, conduct risk, etc. as a risk type and the description)	*(e.g., Low)*	*(e.g., Medium)*	*(e.g., Low)*
…			
…			

Children face a myriad of risks online that may result in harm to children's rights, well-being and development. In this regard, the Organisation for Economic Co-operation and Development (OECD) has published a risk model which highlights the main risks faced by children in the digital environment, for example, content risks, conduct risks, contact risks, consumer risks, and cross-cutting risks (i.e., advanced technology risks, health risks, and privacy risks)[22]. The Institute of Electrical and Electronics Engineers (IEEE) has also outlined several examples of online risks that

[22] OECD, *supra* note 1; Livingstone, *supra* note 1.

children can face when the OECD model is applied, *inter alia* based on the features that a platform may have[23]. Digital service providers would be best placed to ascertain the potential risks and harms to children, and their rights and well-being from their services.

For a further elaboration of the risks and harms faced by children online, please see the introduction to Section 3 of the report on Mapping age assurance typologies and requirements.

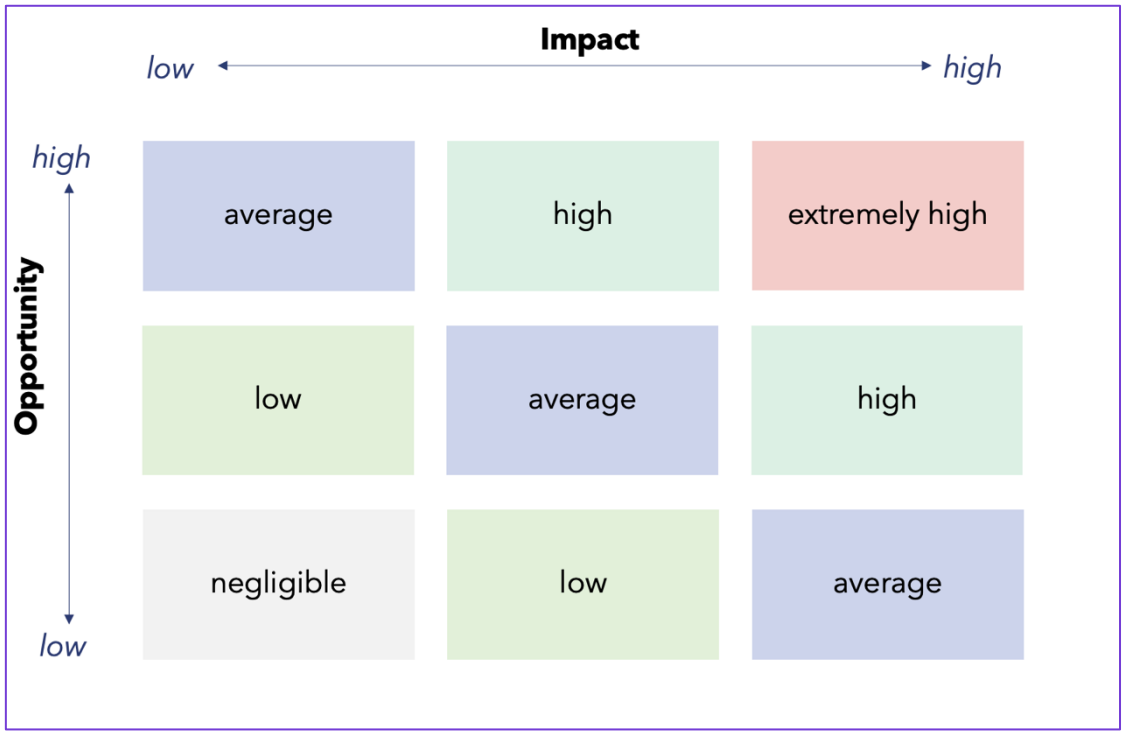
The aforementioned OECD model and IEEE example can be used as guidance for understanding and elaborating on the risks that a digital service can pose to children (first column in the table under question 1.2). For instance, a digital service may host content inappropriate to children of certain ages, and this could pose a content risk to such children. These risks are influenced by factors such as the design and operation of the digital service, the nature of its user base, the nature of content hosted on the digital service, and so on.[24] The description of the digital service provided in response to question 1.1 above can be helpful in identifying these risks. If such risks have already been analysed through assessments such as a CRIA, the same can be used and reproduced here.

To calculate the risks posed by a digital service, estimate the risk by multiplying (i) the probability of a given risk occurring and (ii) the impact if the risk materialises (second and third columns, respectively, in the table under question 1.2). This can provide the final risk assessment (fourth column in the table under question 1.2).

[23] IEEE, *supra* note 6 at 42-47.

[24] GCHQ, *supra* note 5 at 15.

The following risk matrix can be used as indicative guidance on how to assess the risks:[25]



This estimate should reflect the risk before mitigation measures have been taken. Through this analysis, the digital service provider can arrive at multiple risks children face and their corresponding risk levels. Each risk posed by the digital service can fall under one of the five risk levels provided in the above matrix – (i) negligible, (ii) low, (iii) average, (iv) high, and (v) extremely high.

If a digital service is uncertain of the exact risk assessed, for example, because the risk is between low and average, assume the higher of the two assessments.

[25] Leiden University & Considerati. (Mar 2023). Children's Rights Impact Assessment. *Ministry of the Interior and Kingdom Relations, Netherlands*. Pg. 15. https://www.nldigitalgovernment.nl/overview/childrens-rights-online/dossier-documenten/childrens-rights-impact-assessment-manual/.

Reporting example:

Type of risk and description	Probability of risk	Impact of risk	Risk assessment
Contact risk: The digital service allows users to engage in anonymous chats with other users, including video chats. This can, for instance, provide an avenue for adults to engage in 'grooming' children, thus exposing children to contact risks. Given the experience of other such digital service providers in the past, while a majority of adult users do not engage in such activities, there is still a non-negligible number of persons who do so. If 'grooming' occurs, it can have a hugely detrimental impact on the well-being of the child.	Average/ medium	High	High

Q1.3 Is there a legal obligation that requires age assurance to be implemented?
(If yes, proceed to Step 2)

…

Based on the preceding analysis in questions 1.1 and 1.2, it is relevant to ascertain whether there is a legal requirement for age assurance and, in particular, age verification to be implemented by the digital service provider. The law sets requirements for performing a legal act or for a minimum age when products or

(certain practices within) digital services may cause harm to children. Within both these categories, age verification is a necessary measure because the law explicitly states so, or the law can only be complied with if it is known whether a user has reached the minimum age set by the law. In this regard:

(i) Laws such as contract law and data protection law have minimum ages set for the performance of legal acts. Since such minimum ages are prescribed, digital service providers could have to verify the age of the user to ascertain if the legal act performed by the user has validity.

Legal illustration: The minimum age for digital consent (consent is one of the legal grounds for processing of personal data), as regulated by Article 8 GDPR, can be determined by member state law within a range from 13 to 16 years. When children do not yet have the legal capacity to consent to the processing of their personal data, service providers need to obtain parental consent. Therefore, age verification is required to know whether a user has reached the minimum age of digital consent to ensure that legally valid consent is obtained for the processing of personal data and, hence, the processing is lawful.

(ii) Laws such as those that regulate the sale of harmful products (for example, alcohol, cigarettes, weapons, and so on) and provision of harmful services (for example, gambling services, services providing violent or pornographic content, and so on), prescribe a minimum age of the user to whom such products or services can be provided.

Legal illustration: Articles 6a and 28b AVMSD oblige EU member states to ensure that audiovisual media service providers and video sharing platforms take appropriate measures to protect minors from audiovisual content that "may impair the[ir] physical, mental or moral development", including by requiring service providers to use age verification tools in a proportionate manner. The most harmful content (gratuitous violence,

pornography, etc.) should be subjected to the strictest measures, such as effective age verification systems.[26]

To give effect to the AVMSD and Irish domestic law, Ireland's CNM has issued a draft Online Safety Code for public consultation, which *inter alia* states that video-sharing platform service providers shall employ age estimation or age verification or other appropriate technical measures to prevent children from viewing age-inappropriate content.[27]

Member states in the EU may have their own laws and regulatory guidance regarding situations where age assurance, and in particular age verification, is legally necessary.

For a further elaboration of age assurance as a legal requirement, please see Section 3.1 of the report on Mapping age assurance typologies and requirements.

Q1.4 Is there a legal duty of care for the online protection of children that may mandate the implementation of age assurance? (If yes, proceed to Step 2)

…

Based on the preceding analysis in questions 1.1 and 1.2, it is relevant to ascertain whether there is a legal duty of care for the online protection of children, for which

[26] euCONSENT. (Sept 2021). *EU Member State Legal Framework*. Pg. 7. https://euconsent.eu/download/eu-member-state-legal-framework/.

[27] CNM, *supra* note 7 at 52-53.

age assurance may be a solution. In this regard, the law may impose a duty on a digital service provider to protect children from online risks. Age assurance may be a relevant measure to provide such protection, though other measures, such as age-appropriate design, age ratings and parental control tools, may be equally effective or appropriate in given contexts.

Legal illustration: Article 28 DSA imposes a duty on online platforms to "*put in place appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors*". Age assurance may be a measure to achieve such a high level of child protection, but it is not mandated by the DSA as the (only) solution.

In addition, Articles 34 and 35 DSA require very large online platforms (VLOPs) and very large online search engines (VLOSEs) to "*diligently identify, analyse and assess any systemic risks*" stemming "*from the design or functioning of their service" and to "put in place reasonable, proportionate and effective mitigation measures, tailored to the specific risks identified*". Such systemic risks include any actual or foreseeable negative effect to respect for the rights of the child enshrined in Article 24 of the Charter or to the protection of minors or serious negative consequences to a person's physical and mental well-being (see Article 34 (1) (b) and (d)). The DSA explicitly states that the necessary mitigation measures, including taking targeted measures to protect the rights of the child, can include age verification (see Article 35 (1) (j) DSA).

Unlike when age assurance is a legal requirement, for the legal duty of care category of cases, it is relevant to determine whether age assurance is a necessary measure in the first place. Age verification, in particular, can be an exclusionary measure (for example, children may be excluded from a service) and should therefore be used with caution.[28]

[28] 5Rights Foundation, *supra* note 5 at 51.

For a further elaboration of age assurance as a legal duty of care, please see Section 3.2 of the report on Mapping age assurance typologies and requirements.

In view of the same, a decision needs to be arrived at regarding the need for age assurance in a proportionate manner. The principle of proportionality is a fundamental principle when limiting the rights of EU citizens, including children. In the present context, proportionality requires that a balance be struck between (a) the means used to achieve the intended objective and (b) its impact on the limitation of the rights of individuals, including children.[29] Part of the proportionality test is to assess whether, of all the available measures that can achieve the intended purpose, does this particular measure interfere the least with the rights of individuals, including children.

Therefore, it is necessary to analyse *whether age assurance is an effective means of achieving the objective,* that is age-appropriate access to goods and services while maintaining the online protection of the rights and well-being of children. In particular, it must be determined whether age assurance can effectively protect children from the risks of the digital service (as identified in question 1.2) while holistically respecting children's rights. If it is determined that age assurance is an effective means of both age-appropriate access to goods and services and protecting (certain groups of) children given the risks, it should be determined whether age assurance is the least invasive way in terms of interference with the rights of individuals, including children, or if there is a way that is equally efficient but less invasive. Invasiveness can involve various aspects, including privacy, inclusiveness, user autonomy and security. Consideration should also be paid to whether other measures, such as age-appropriate design, age ratings and parental

[29] European Data Protection Supervisor. (n.d.). *Necessity & Proportionality*. https://edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality_en.

control tools, may be more appropriate and less invasive than age assurance for achieving a proportionate outcome.

For a further elaboration of the requirement of proportionality while implementing age assurance, please see Section 5.1 of the report on Mapping age assurance typologies and requirements.

Reporting example: The digital service presents a content risk to children, whereby children can be exposed to viewing age-inappropriate content shared by other users. Based on the analysis made, the risk is categorised as a high-level risk. In order to protect children from this risk while continuing to provide them with the appropriate services, age assurance is seen as a necessary and proportionate measure, in conjunction with other measures such as age ratings and parental control tools.

Q1.5 Is there any other reason for the implementation of age assurance? (If yes, proceed to Step 2)

…

Based on the preceding analysis in questions 1.1 and 1.2, it is relevant to ascertain whether any other reasons (apart from those discussed in questions 1.3 and 1.4) exist that necessitate considering the implementation of age assurance. For instance, there could be a contractual provision in the terms and conditions of the digital service that states that the user must be of a certain minimum age to access and use the digital service, based on which age assurance may be required. There may also be situations where there is no legal or contractual stipulation for age assurance, but a digital service provider still arrives at an assessment that, given the risks posed by the digital service to the online safety of children, age assurance may be a relevant mitigation measure.

For a further elaboration of age assurance as a contractual obligation or as a voluntary decision, please see Sections 3.3 and 3.4 of the report on Mapping age assurance typologies and requirements.

In these situations, similar to the legal duty of care category of cases in question 1.4, it is relevant to determine whether age assurance is a necessary measure in the first place. Given the potential exclusionary impact of age assurance, a proportionate decision has to be taken on the need for age assurance given the risks posed by the digital service (as identified in question 1.2). Please see the discussion above under question 1.4 on making proportionate decisions regarding the necessity of age assurance.

Step 2 – Determining the level of assurance

Once it is determined under Step 1 that age assurance is to be implemented, the next step is to determine what assurance level is required for the age assurance process of the digital service. Without a sufficient assurance level, age assurance will not effectively mitigate the risks posed to children. The more accurate the age assurance process is, the lower the likelihood for children to access and use (parts of) digital services that may be harmful to them, or for users not to be granted access to a digital service despite having met the minimum age requirement.

Q2 What level of assurance does the age assurance process to be implemented need to provide?

…

There are different types of age assurance methods available (as elaborated further under Step 3), and these have varying levels of assurance. There are various views present in the literature regarding the assurance levels of particular methods,[30] and there have been initiatives to quantify the accuracy of age assurance methods in certain contexts as well.[31]

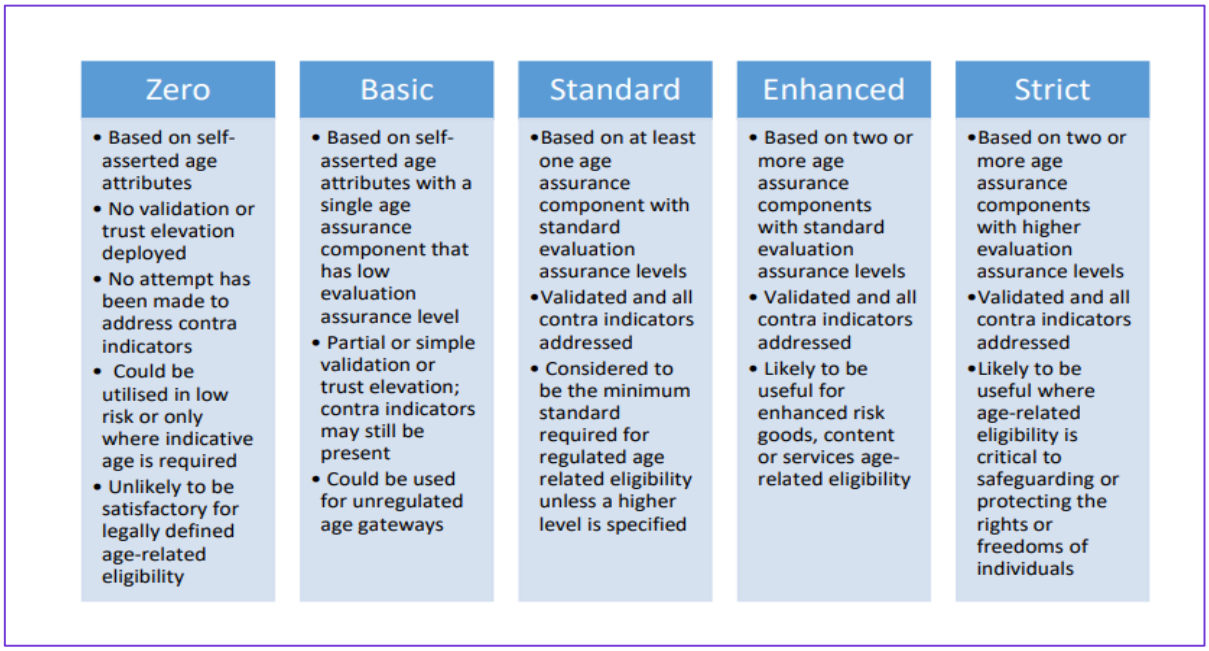
There have also been certain initiatives to propose a mechanism to determine the confidence one can have regarding the accuracy of age assurance processes. Further clarity may be achieved regarding this aspect as more work on age assurance is undertaken by organisations in the future.

[30] For instance, 5Rights Foundation, supra note 5; UNICEF, supra note 5; eSafety Commissioner, Australia. (Aug 2023). *Roadmap for age verification and complementary measures to prevent and mitigate harms to children from online pornography*. https://www.esafety.gov.au/sites/default/files/2023-08/Age-verification-background-report.pdf.

[31] ACCS. (2022). Measurement of Age Assurance Technologies. https://ico.org.uk/media/about-the-ico/documents/4021822/measurement-of-age-assurance-technologies.pdf; NIST. (n.d.). Face Analysis Technology Evaluation (FATE) Age Estimation & Verification. https://pages.nist.gov/frvt/html/frvt_age_estimation.html.

For a further elaboration of the mechanisms proposed to categorise confidence on age assurance, please see the third part of Section 4.2 of the report on Mapping age assurance typologies and requirements.

For the purpose of this self-assessment tool, a five-level classification of assurance levels of age assurance processes can be followed. The International Organization for Standardization (ISO) working draft on age assurance proposes a five-level zero-basic-standard-enhanced-strict confidence model[32] for age assurance (see figure below), which can be useful:



ISO's five-level approach has also been adopted by organisations such as the Age Check Certification Scheme (ACCS).[33] However, this self-assessment tool does not wholly adopt the classification proposed in the ISO working draft and the various

[32] ISO, *supra* note 16 at 13-16.

[33] ACCS, *supra* note 31 at 15.

parameters mentioned therein, as it is still a work in progress that is undergoing revisions.[34]

This self-assessment tool merely provides guidance on a five-level assurance classification to match the five broad categories of risk levels explained earlier in question 1.2. Consequently, the following matrix shows how the indicative guidance on the level of assurance corresponds to the risk assessment:

Risk assessment	Level of assurance
No/negligible	Zero/negligible
Low	Low/basic
Average	Average/medium/standard
High	High/enhanced
Extremely high	Extremely high/strict

On the one hand, this approach can ensure a flexible approach for digital service providers to use assurance levels based on the given context. For instance, digital service providers may decide to use a three-level low-medium-high confidence model, such as the one proposed by the UK's GCHQ (Government Communications Headquarters),[35] if that better fits the context in which they operate. On the other hand, this approach can also provide a foundation to potentially use a five-level assurance model (with specific parameters) across the age assurance industry in a standardised manner, if and when standards towards this end are finalised.

[34] *See* ISO, *supra* note 6.

[35] GCHQ, *supra* note 5 at 18-19.

It is worth mentioning that these are broad assurance levels laid out above, which can change depending on the context in which a digital service operates. The present self-assessment tool does not contain detailed guidance on how to assess the assurance levels of given age assurance methods or processes, as there are currently no agreed-upon parameters for such assessments. Equally, such determinations vary widely depending on the technology and context of deployment.

Step 3 – Formulating a proportionate age assurance process

Once it is determined that age assurance of an identified assurance level is necessary (Steps 1 and 2), it must be determined which age assurance tool(s) is (are) to be employed as part of the age assurance process. There are several methods of age assurance that are present today, and still more that may come to fruition in the near future. Some of these age assurance methods are: (1) Self-declaration; (2) Hard identifiers; (3) Credit cards; (4) Self-sovereign identity; (5) Account holder confirmation; (6) Cross-platform authentication; (7) Facial age estimation; (8) Behavioural profiling; (9) Capacity-testing; and (10) Third-party age assurance services.

The above is not an exhaustive list of age assurance methods present today, and methods such as checking age against data held by entities, including banks, are also used in certain countries.[36] Other methods, including estimation techniques using voice analysis could also become prominent in the future.[37] EUDI wallets envisaged under the European Digital Identity regulation[38] will also become a method going forward. Each of these methods has varying assurance levels and associated advantages and disadvantages.

Within each of these methods, there are various age assurance tools, and the actual characteristics and issues of particular age assurance tools depend on the context of deployment and the specific design of these tools. It is also worth mentioning that digital service providers may use a combination of age assurance

[36] 5Rights Foundation, *supra* note 5 at 26; euCONSENT. (02.01.2022). *D2.2 EU Methods for AVMSD and GDPR Compliance Report*. Pg. 9-10. https://euCONSENT.eu/project-deliverables/.

[37] ICO, *supra* note 15 at 9; euCONSENT, *supra* note 36 at 11.

[38] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework. OJ L 2024/1183, 30.4.2024.

tools instead of relying on any single tool,[39] which can potentially increase the level of assurance.

For a further elaboration of the types of age assurance and their characteristics, please see Section 4.1 and the first part of Section 4.2 of the report on Mapping age assurance typologies and requirements.

The questions in Step 3 can be used to guide the digital service provider in opting for the appropriate age assurance process given the context of their operations.

Q3.1 Which age assurance tool(s) provide(s) the required level of assurance?

…

The level of assurance required of the age assurance process (as identified in Step 2) is a primary guiding factor behind determining which tool(s) of age assurance is (are) to be implemented. As mentioned in Step 2, there are several initiatives underway that seek to lay down parameters for accuracy of age assurance methods. The accuracy of age assurance tools depends on the underlying technology and can also depend on factors such as whether the age assurance tool effectively addresses different human characteristics (for example, gender, race or ethnicity),[40] different circumstances of use (for example, light or dark setting) and

[39] 5Rights Foundation, *supra* note 5 at 45.

[40] ACCS, *supra* note 31 at 24.

how easily the tool can be circumvented by users (as further elaborated in Step 4.5).

Other relevant factors to consider in identifying the appropriate age assurance tool(s) could be the age assurance products available in the market, the technical capabilities and resources of the digital service, the cost and technical feasibility of available products, and so on. However, costs and technical considerations should not be used as routine justifications for not employing appropriate age assurance. If it is not possible to implement age assurance processes of the required assurance level (where it is not legally mandatory to do so), it should be demonstrated why this is the case (for example, technical explanations, disproportionate costs, disproportionate impact on other users, and so on).[41] Based on such a holistic consideration, the digital service provider can identify potential age assurance tool(s) for implementation. This process may identify multiple age assurance tools that, when used in combination, provide the required assurance level and can also be practically implemented by the digital service provider.

Q3.2 What are the advantages and disadvantages associated with the identified age assurance tool(s)?

…

The various methods of age assurance have their own advantages and disadvantages, as well as varying assurance levels, as outlined in question 3.1. In view of the same, the digital service provider can assess how the identified age assurance tool(s) fare in the following parameters (questions 3.2.1- 3.2.5) to assist in choosing the best possible option. It bears mention that this is not an exhaustive list of parameters, and there could be other relevant factors depending on the

[41] ICO, *supra* note 15 at 11.

context. Further, it is possible that the identified tool(s) of age assurance may have no impact on some of these parameters.

Q3.2.1 How does the age assurance tool perform with respect to privacy and data protection requirements?

…

Age assurance methods may involve the processing of personal or sensitive data of users (including minors), and age assurance providers must then comply with the legal provisions of the General Data Protection Regulation (GDPR).[42] In this regard, regulators such as the Irish Data Protection Commission (DPC) and the UK's Information Commissioner's Office (ICO) have clearly stated that data protection principles as enshrined in Article 5 GDPR (data minimisation, accuracy, storage limitation, etc.) ought to be paid due consideration while employing age assurance.[43] If biometric data is used, then conditions for processing special categories of data as provided in Article 9 GDPR may also need to be met.[44]

If any issues, especially (potential) risks related to privacy and data protection, are identified in answering this question, users of this self-assessment tool should mention these in response to question 3.3 below.

[42] Brennen, S., & Perault, M. (2023). Keeping Kids Safe Online: How Should Policymakers Approach Age Verification?. *The Center for Growth and Opportunity*. Pg. 8. https://www.thecgo.org/research/keeping-kids-safe-online-how-should-policymakers-approach-age-verification/.

[43] ICO, *supra* note 15 at 21-28; DPC. (Dec 2021). *Fundamentals for a Child-Oriented Approach to Data Processing*. Pg. 48. https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf.

[44] ICO, *supra* note 15 at 29-30.

For a further elaboration of privacy as a requirement for age assurance, please see Section 5.2 of the report on Mapping age assurance typologies and requirements.

Reporting example: The identified age assurance tool analyses hard identifiers by giving users the option to upload a scanned copy of the document along with a selfie of themselves holding the document in a legible manner so as to confirm that the document belongs to the user. This can have an impact on the privacy rights of the users, as personal data (including biometric data) could be collected for the purpose of age verification. There are also added concerns such as whether the principles of data minimisation and storage limitation as enshrined in Article 5 GDPR are met.

Q3.2.2 How does the age assurance tool perform with respect to security requirements?

…

Age assurance could involve the processing of personal data, and it is therefore important that age assurance systems are secure and prevent unauthorised access to the data processed.[45] Age assurance systems must also have sufficient cybersecurity measures to ensure that their functioning is not compromised to the detriment of children, other users and digital services.

If any issues, especially (potential) risks related to security, are identified in answering this question, users of this self-assessment tool should mention these in response to question 3.3 below.

[45] CEN, *supra* note 12 at 27.

For a further elaboration of security as a requirement for age assurance, please see Section 5.3 of the report on Mapping age assurance typologies and requirements.

Q3.2.3 Is the age assurance tool functional and easy to use?

...

It is imperative that age assurance technologies are easy to use in order to further their adoption and avoid unnecessary burdens on the users.[46] Further, the age assurance technologies employed must offer functionality which is appropriate to the capacity and age of the child using such technologies,[47] in line with the evolving capacities of the child principle as enshrined in Article 5 UN CRC.

If any issues, especially (potential) risks related to functionality and ease of use, are identified in answering this question, users of this self-assessment tool should mention these in response to question 3.3 below.

For a further elaboration of functionality and ease of use as a requirement for age assurance, please see Section 5.5 of the report on Mapping age assurance typologies and requirements.

Reporting example: The identified age assurance tool employs facial analysis technology to conduct facial age estimation. The analysis is conducted at the entry point of the digital service. As the facial age estimation is performed within a short

[46] 5Rights Foundation, *supra* note 5 at 49.

[47] CEN, *supra* note 12 at 27.

span of time and a decision to grant or deny access is instantly made, the identified age assurance tool appears to fare well with respect to functionality and ease of use for the users.

Q3.2.4 Is the age assurance tool inclusive, and does it not unfairly exclude users?

...

Non-discrimination, as enshrined in Article 2 of the United Nations Convention on the Rights of the Child (UN CRC), is one of the four general principles of the UN CRC and requires that effective access to the digital environment be provided to children and that digital exclusion of children is prevented.[48] Particular consideration must be given to children who face challenges in relation to digital accessibility, such as children with intellectual and/or physical disabilities or children not having access to particular age assurance methods or tools.[49] Additionally, other factors that may impact the inclusiveness of the age assurance process for users, including children, such as language, skills and socioeconomic status, must be appropriately addressed,[50] *inter alia* by relying on applicable laws and standards.[51]

If any issues, especially (potential) risks related to inclusivity and non-discrimination, are identified in answering this question, users of this self-assessment tool should mention these in response to question 3.3 below.

[48] Committee on the Rights of the Child. (02.03.2021). *General comment No. 25 (2021) on children's rights in relation to the digital environment*. CRC/C/GC/25. Pg. 2. https://digitallibrary.un.org/record/3906061?ln=en.

[49] *Ibid* at 15.

[50] 5Rights Foundation, *supra* note 5 at 51.

[51] Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services, OJ L 151, 7.6.2019, p. 70–115; ETSI. (Mar 2021). *Accessibility requirements for ICT products and services*. EN 301 549. https://www.etsi.org/deliver/etsi_en/301500_301599/301549/03.02.01_60/en_301549v030201p.pdf.

For a further elaboration of inclusivity and non-discrimination as a requirement for age assurance, please see Section 5.6 of the report on Mapping age assurance typologies and requirements.

Q3.2.5 Does the age assurance tool further user participation and access to the digital service?

...

Age assurance should support age-appropriate access to goods and services and should not result in unduly blocking children from accessing a digital service or in providing children with an inferior quality of a digital service.[52] Age assurance, though intended to protect children from harm, should also respect their participatory rights, for instance, by supporting age-appropriate design of (parts of) the service.[53] Providing children access to digital services is of vital importance because the right to participate in society is enhanced by and increasingly dependent on digital services.[54]

If any issues, especially (potential) risks related to furthering participation and access, are identified in answering this question, users of this self-assessment tool should mention these in response to question 3.3 below.

[52] DPC, *supra* note 43 at 45.

[53] 5Rights Foundation, *supra* note 5 at 49.

[54] Assim, U. M. (2019). Civil Rights and Freedoms of the Child. In U. Kilkelly & T. Liefaard (Eds.), *International Human Rights of Children* (p. 389–417). Springer. Pg. 398. https://doi.org/10.1007/978-981-10-4184-6_7.

For a further elaboration of furthering participation and access as a requirement for age assurance, please see Section 5.7 of the report on Mapping age assurance typologies and requirements.

Q3.3 What are the (potential) risks posed by the identified age assurance tool(s)?

Type of risk and description	Probability of risk	Impact of risk	Risk assessment
(e.g., privacy risk, security risk etc. as a type and the description)	*(e.g., Medium)*	*(e.g., High)*	*(e.g., High)*
…			
…			

Based on an assessment of the benefits and drawbacks of identified age assurance tool(s) under question 3.2, a clearer picture of the (potential) risks of the age assurance tool(s) should be available. Here, these risks are explicitly identified. For example, an age assurance tool involving behavioural profiling may pose a risk to the privacy of all users, including children. The risk matrix provided under question 1.2 may again be used to identify and assess risks more specifically, such as risks to privacy, security, and so on. These risks should be identified and assessed without accounting for potential mitigation measures.

Q3.4 Are there mitigation measures to combat the (potential) risks from the identified age assurance tool(s)?

Type of risk and description	Risk assessment	Measures	Residual risk
(e.g., privacy risk, security risk etc. as a type and the description)	*(e.g., High)*	*(e.g., Immediate data deletion)*	*(e.g., Low)*
…			
…			

Based on an assessment of the benefits and drawbacks as well as (potential) risks of identified age assurance tool(s) as undertaken in response to questions 3.2 and 3.3, it can be assessed what measures could be implemented to mitigate these risks. For instance, if there is a privacy risk, then implementing on-device solutions could mitigate the risk and reduce the risk level to arrive at a residual risk. Ascertaining the potential mitigation measures and consequent residual risk is important in guiding the decision-making under question 3.5.

Q3.5 Which identified age assurance tool(s) is (are) the proportionate solution for the age assurance process to be implemented?

…

This is the stage where, based on a holistic consideration of the identified age assurance tool(s) in response to questions 3.1 to 3.4, the digital service provider can decide on the proportionate age assurance process for their digital service. This determination should be done in accordance with the principle of proportionality (as elaborated under question 1.4). Again, this requires an analysis of whether the age

assurance process achieves the objective (for example, establishing age to a given level of assurance that corresponds to the risk level) in a proportionate manner (for example, whether it is the least invasive method given the other requirements discussed under question 3.2). Given the context and age assurance state of the art, requirements discussed under question 3.2 may conflict with the desired level of assurance. For instance, increasing accuracy might negatively impact privacy in a situation where hard identifiers are proposed as the age assurance method. The purpose of the analysis should be to arrive at balanced decision-making considering a given context and the proportionality principle.

For a further elaboration of the requirement of proportionality while implementing age assurance, please see Section 5.1 of the report on Mapping age assurance typologies and requirements.

Depending on the situation, the digital service provider may decide on one age assurance tool or alternative age assurance tools for users to choose from. Digital service providers can also combine age assurance tools to achieve greater or lesser levels of certainty in the age that the user claims to be (claimed age). In this case, age assurance activities are performed sequentially, and the next activity depends on the output of a previous activity. This is also known as the 'waterfall technique'.[55] For instance, the use of a facial age estimation tool can be combined with a capacity testing tool to give greater certainty regarding the claimed age if outputs align, and lesser certainty regarding the claimed age if different outputs are generated.

Thus, as previously mentioned, using a combination of age assurance tools could ultimately increase the level of assurance. The consideration of proportionality should be based on this entire age assurance process envisaged by the digital

[55] ACCS, *supra* note 31 at 36-37.

service provider, where the age assurance process may include one or more age assurance tools.

It is also possible in a given situation that, after considering questions 3.1 to 3.4, a digital service provider may conclude that the decision on question 1.4 or 1.5 (that age assurance needs to be implemented as a mitigating measure) was incorrect. This may be due, in part, to the fact that age assurance may not be a proportionate measure for online child safety, if implemented using the available age assurance tools. In such a situation, subject to legal obligations, a digital service provider would need to revisit questions 1.4 or 1.5 and reconsider their decision. A similar reconsideration of the desired level of assurance as determined in question 2 may also be needed.

Step 4 – Implementing the age assurance process

Step 4 helps a digital service provider implement age assurance in a more effective and rights-respecting manner. The aspects to be considered in Step 4 are not hierarchical, and it is possible that some of them may have already been considered in the analysis under Step 3. It is also possible that some of these aspects are not applicable in a given situation and that other aspects not mentioned in Step 4 need to be considered instead or in addition, as the age assurance technologies and initiatives relating to it further develop.

While implementing the age assurance process, the digital service provider should ascertain whether the following aspects are paid due consideration:

Q4.1 What is the stage at which age assurance is conducted?

…

Digital service providers determine at what stage of the user journey on the digital service the user will be faced with the age assurance process. It may be that age assurance is implemented at the point of entry of the digital service before any part of the service or content is accessed. It can also be the case that age assurance is implemented at certain other trigger points within the digital service (for example, when engaging in live chat with other users or moving from a mixed-age setting to an 18+ setting).

Q4.2 What is the duration for the validity of age assurance decisions, and how often is age assurance to be repeated?

…

Digital service providers determine the period for which a user's age determination is valid and how often age assurance should be performed for a given user. While repeatedly performing age assurance may further accuracy, it can negatively affect privacy and functionality for the user.

Q4.3 What is the specified age format?

…

Digital service providers determine what data relating to a user's age is to be collected and retained. For instance, digital service providers need to decide if the data should include the date of birth, age, age range or merely sufficiency of age. Such a determination can be helpful in achieving data minimisation by preventing the processing of unnecessary data.

It can also be useful for digital service providers to decide on implementing an 'age buffer', that is having a buffer range around the age sufficient for using a digital service (this is a more relevant consideration when age assurance is legally prescribed and age estimation is used).[56] For instance, when the age of 18+ years is required to use the digital service, the age estimation process approves only users estimated to be at least 21 years of age, thus providing a margin of error (buffer) to mitigate false positives.[57] This could allow digital service providers to use age verification tools for a smaller portion of their user base (those falling in the buffer range) instead of for the entire user base,[58] particularly when age verification tools are construed to be relatively privacy- or otherwise invasive. Thus, digital service providers can determine aspects relating to the age buffer (if used),

[56] *Ibid* at 40.

[57] ISO, *supra* note 16 at 4.

[58] IEEE, *supra* note 6 at 24-25.

such as what the buffer range is, and what is the resolution (or alternative option) provided to those estimated to be in the buffer range. It is important to be cautious while administering an age buffer given the potential exclusionary effects it can have on users of sufficient age.

Q4.4 What is the level of authentication required?

…

Authentication is the process by which digital service providers determine whether a user's verified or determined age can be sufficiently attributed to the user (for example, when they log in again) before they are granted access to the digital service.[59] Authenticators are generally used to ascertain this, and authenticators can be:

- something the user knows (e.g., PIN, password),
- something the user has (e.g., age token, credit card),
- something the user is (e.g., biometric, signature).[60]

Thus, digital service providers determine what the authentication processes for age assurance are and how frequently authentication is required. It should be considered that stricter and more frequent authentication requirements can increase the accuracy of age assurance processes but could negatively affect users' experiences of the service's functionality.

[59] *Ibid* at 40-41.

[60] ACCS, *supra* note 31 at 50-51.

Reporting example: The digital service provider conducts the initial age assurance through facial age estimation technology. Eligible users are asked to generate a password, which is then used to access their account.

Q4.5 Have circumvention techniques been addressed?

…

Various techniques allow users to circumvent age assurance tools. For instance, individuals may use computer programs to evade a remote age assurance tool (known as the 'liveness' issue).[61] Users may capture data or information from external sources (for example, a facial image) and present that to age assurance tools as their own (known as the 'presentation attack' issue),[62] and deepfakes may also be used to circumvent age assurance methods such as facial age estimation.[63] Children may also collude with adults to circumvent age assurance methods, for example, by using an adult's credit card. Thus, digital service providers must ascertain the potential circumvention techniques for the age assurance process and how they can be addressed. As mentioned in Step 3.1, the ease with which an age assurance tool can be circumvented can play a role in the accuracy of the same.

Q4.6 Have contra-indicators been addressed?

…

[61] ISO, *supra* note 16 at 17.

[62] *Id*; ACCS, *supra* note 31 at 53-54.

[63] Arcom, *supra* note 7 at 12.

Contra-indicators refer to mismatches of data or information showing that the claimed age may not be true[64], for instance, different dates of birth entered by the user at two different stages of age assurance. The ability of an age assurance process to combat such false claims is relevant for the overall level of assurance.[65] Therefore, when such contra-indicators exist, additional evidence may need to be gathered to ascertain the veracity of the claimed age.[66] Thus, digital service providers must ascertain how potential contra-indicators can be addressed in the age assurance process.

Reporting example: The digital service provider uses a combination of facial age estimation and behavioural profiling to conduct age assurance. It is noticed that the algorithmic estimation based on the behavioural profiling technology is markedly different from the age range initially reflected through the facial age estimation method. In order to address this discrepancy, the user is asked to prove his age through hard identifiers.

Q4.7 Should interoperable age assurance solutions be provided?

…

Interoperability in an age assurance context means allowing users to re-use completed age assurance decisions from trusted third parties providing age assurance services with other digital service providers,[67] by sharing only the attribute of age with the latter.[68] Digital service providers may determine whether

[64] ISO, *supra* note 16 at 18.

[65] IEEE, *supra* note 6 at 40.

[66] ISO, *supra* note 16 at 18.

[67] Ofcom, *supra* note 7 at 26.

[68] IEEE, *supra* note 6 at 27.

such functionality shall be provided and which third parties can be considered trustworthy based on industry-accepted norms and standards. Other relevant factors, such as privacy and security, must also be considered while providing interoperability. Achieving interoperability among age assurance solutions can help tackle the issue of user functionality being affected by the frequent use of different age assurance methods by digital service providers, requiring users to constantly perform a multitude of actions to prove their (minimum or maximum) age.[69] Efforts to achieve interoperability have already been spearheaded by initiatives such as euCONSENT.[70] EU-wide initiatives such as the EUDI wallets[71] should also help foster interoperability in the age assurance sphere in the future.

Q4.8 Is only personal data processed that is necessary to perform age assurance?

...

Data minimisation, purpose limitation, and storage limitation are some of the fundamental data protection principles enshrined in Article 5 GDPR. While it goes without saying that age assurance processes should comply with these and other data protection principles, digital service providers should make substantial efforts to safeguard these carefully and diligently. Only data strictly necessary to perform the age assurance process should be processed. Moreover, data should not be sold or shared further.[72] All other user data collected during age assurance, which is not required for age assurance processes or regulatory compliance, should be deleted.

[69] Brennen, *supra* note 42 at 8.

[70] euCONSENT, (n.d.). *EUCONSENT. ELECTRONIC IDENTIFICATION AND TRUST SERVICES FOR CHILDREN IN EUROPE. Creating a safer digital world for children throughout the European Union*. https://euCONSENT.eu/.

[71] European Commission. (n.d.). *A digital ID and personal digital wallet for EU citizens, residents and businesses*. https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/EU+Digital+Identity+Wallet+Home.

[72] 5Rights Foundation, *supra* note 5 at 49.

For instance, if a scanned copy of a hard identifier document is obtained from the user, it would contain data in addition to the user's age, which must not be retained (unless required by regulatory stipulations). Furthermore, it should be considered whether personal data related to age should be kept at all or whether it is sufficient to log that the age assurance process was successful and what the result was (for example, a yes/no response to whether the user has the required minimum or maximum age).

Q4.9 Have the users received transparent information on the age assurance process implemented?

…

Digital service providers should provide users with adequate and intelligible information regarding the age assurance process and its operation.[73] When such information is provided to children, digital service providers should present information relating to age assurance in an attractive, understandable and recognisable manner tailored to the age of the young users accessing their service,[74] while appreciating the evolving capacities of children under Article 5 UN CRC. Particularly, adding formats that may be attractive to children, such as chatbots, videos, games, or comics, may help get the information across.[75]

[73] CEN, *supra* note 12 at 10; BSI. (31.03.2018). *PAS 1296:2018 Online age checking. Provision and use of online age check services. Code of Practice*. Pg. 12.

[74] ACCS. (2021). *Technical Requirements for Age Appropriate Design for Information Society Services*. Pg. 29. https://ico.org.uk/media/for-organisations/documents/2620427/accs-3-2021-technical-requirements-aadc.pdf.

[75] *See* on child-friendly transparency, Milkaite, I., & Lievens, E. (2020). Child-friendly transparency of data processing in the EU: from legal requirements to platform policies. *Journal of Children and Media*, *14*(1), 5-21. Pg. 16-17.

For a further elaboration of transparency as a requirement for age assurance, please see Section 5.8 of the report on Mapping age assurance typologies and requirements.

Q4.10 Have the users been provided sufficient avenues against incorrect age assurance decisions?

...

Digital service providers should follow due process regarding age assurance decisions. If the implemented age assurance process incorrectly determines the age of the users, users should have recourse against such determination.[76] This should be enabled by having an easy and expedient mechanism to challenge age assurance decisions and seek redress against it.[77] Even if the user only wants to notify digital service providers of an incorrect decision, there must be an easy-to-use avenue.

For a further elaboration of notification, challenge and redressal mechanisms as a requirement for age assurance, please see Section 5.9 of the report on Mapping age assurance typologies and requirements.

Reporting example: The digital service provider employs capacity testing as the age assurance method and users who have been declared to be of insufficient age

[76] Brennen, *supra* note 42 at 8.

[77] 5Rights Foundation, *supra* note 5 at 50.

are notified about this through a layered notice, along with corresponding remedies they can take. The remedies include challenging the age assurance decision by seeking age assurance through conducting age estimation via a live video feed by personnel of the digital service provider. This decision can be appealed to a higher-level officer in the company, and adequate proof of age through hard identifiers can be provided.

Q4.11 Are third-party age assurance providers engaged and have been made adequately aware of the age assurance requirements?

...

Digital service providers can use the services of third-party age assurance providers to provide an assurance of age or to confirm the identity of the users.[78] In fact, certain regulators, such as the French Arcom (Regulatory Authority for Audiovisual and Digital Communication), envisage that digital service providers that host pornographic content should perform age verification only through an independent third party.[79] In all cases where a third-party age assurance provider is engaged, it is relevant that digital service providers ensure these third parties adhere to the requirements for age assurance identified by the digital service provider. Further, digital service providers have to convey relevant information to the third party based on the given fact situation. This can be information regarding the level of assurance expected, the method of age assurance to be employed, how to deal with contra-indicators, and so on. The primary responsibility for ensuring appropriate age assurance is generally with the digital service providers themselves.

[78] 5Rights Foundation, *supra* note 5 at 34.

[79] Arcom, *supra* note 7 at 16.

When third parties are involved in the age assurance process, there are also additional considerations to be kept in mind such as how the communication regarding the user's age is transmitted by the third party to the digital service provider, and what personal data is processed by the third party for performing age assurance. [80] Paying attention to these aspects can help ease concerns relating to surveillance of a user's online behaviour when third parties are present.[81]

For a further elaboration of the use of third-party age assurance services, please see Section 4.10 and the second part of Section 4.2 of the report on Mapping age assurance typologies and requirements.

[80] Sas, M., & Mühlberg, J. T. (2024, February). Trustworthy Age Assurance?. In *The Greens Cluster: Social & Economy, Location: The European Parliament*. Pg. 68-69. https://www.greens-efa.eu/en/article/document/trustworthy-age-assurance.

[81] *Id.*

Step 5 – Monitoring the adequate performance of the age assurance process

In Step 5, the digital service provider reviews both the digital service and the age assurance process that has been implemented and assesses whether the performance of the process is as required and anticipated.

Q5.1 Is the age assurance process performing as expected?

…

The expectations based on decisions made in Steps 1 to 4 are analysed against the actual performance of the process. Factors to be analysed are, among others, whether the assurance level is correct and being achieved, and whether the age assurance tool(s) are appropriate and performing adequately with respect to privacy and functionality. For instance, the ongoing use of the digital service can reveal an unforeseen risk to children that requires a revaluation of the desired assurance level for age assurance.

Industry-accepted conformity assessments and adherence to standards concerning age assurance methods and processes can be useful parameters for performing this monitoring. If a third party is engaged, the digital service provider must assess whether the third party is providing all the relevant information to allow the digital service provider to ascertain the proper functioning of the age assurance process. The digital service provider must decide how often the age assurance process will be assessed.

Q5.2 Is there any other factor that requires revisiting the age assurance choices?

…

Other factors may require revising the age assurance choices made in Steps 1 to 4. These factors can include regulatory developments, technological developments, external reports pertaining to the user base, and customer feedback. For instance, new age assurance products that provide better privacy features than the age assurance process currently used may become available. Digital service providers should be open to reconsidering age assurance choices based on such factors.

Q5.3 Are records and documentation relating to the implementation of the age assurance process complete and up-to-date?

…

Digital service providers may find it helpful to formulate a statement, report or policy which contains the decisions made by digital service providers regarding implementing the age assurance process.[82] Other underlying documents, such as contracts and communications with third-party age assurance providers, performance indicators of age assurance employed, and so on, can also be maintained to show compliance with the applicable law.

[82] A similar concept termed as 'age check practice statement' is mentioned in PAS 1296:2018. *See* BSI, *supra* note 73 at 9, 44-48. It is also termed as 'age assurance practice statement' in the IEEE Approved Draft Standard. *See* IEEE, *supra* note 6 at 23-24.

Relevant cross-cutting considerations

A. Have children and other relevant stakeholders been sufficiently consulted regarding the implementation of the age assurance process?

…

Children have a right to be heard under Article 12 UN CRC, which is a fundamental principle of the UN CRC, and digital service providers should appropriately engage with children and pay due attention to their views.[83] Digital service providers should empower children to exercise this right by allowing them to convey their views on age assurance and, particularly, the implementation of the age assurance process. Digital service providers can, for instance, engage with policy bodies that work with children and conduct online surveys, social media polls, and similar, to hear children's views. The views of children and other stakeholders (including parents and other users) are relevant in informing the digital service provider of the risks posed (as addressed in response to question 1.2), the age assurance process to be implemented (as addressed under Step 3), the functionality of age assurance tools, and so on. There are therefore various stages where such useful inputs can be sought.

For a further elaboration of hearing the views of children as a requirement for age assurance, please see Section 5.10 of the report on Mapping age assurance typologies and requirements.

[83] Committee on the Rights of the Child, *supra* note 48 at 3.

B. Is age assurance compliant with relevant legislation in relation to data protection and privacy, harmful content, platform regulation, and so on?

…

Ensuring legal compliance when providing online services, including age assurance, is an equally obvious and vital requirement. As explained under questions 1.3 and 1.4, EU legislation, such as the GDPR, the AVMSD and the DSA, may be applicable to digital services and the implementation of the age assurance process, in addition to the member state-specific legislation. Legal compliance is required at various stages of the age assurance process, and digital service providers should be aware of this, as well as of relevant new legal developments (for example, the proposed Cyber Resilience Act, 2022).[84]

[84] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, COM(2022) 454 final, (15.09.2022).

Bibliography

5Rights Foundation. (Oct 2021). *But how do they know it is a child? Age Assurance in the Digital World*. https://5rightsfoundation.com/uploads/But_How_Do_They_Know_It_is_a_Child.pdf.

Age Check Certification Scheme. (2021). *Technical Requirements for Age Appropriate Design for Information Society Services*. https://ico.org.uk/media/for-organisations/documents/2620427/accs-3-2021-technical-requirements-aadc.pdf.

Age Check Certification Scheme. (2022). *Measurement of Age Assurance Technologies*. https://ico.org.uk/media/about-the-ico/documents/4021822/measurement-of-age-assurance-technologies.pdf.

Assim, U. M. (2019). Civil Rights and Freedoms of the Child. In U. Kilkelly & T. Liefaard (Eds.), *International Human Rights of Children* (p. 389–417). Springer. https://doi.org/10.1007/978-981-10-4184-6_7.

Brennen, S., & Perault, M. (2023). Keeping Kids Safe Online: How Should Policymakers Approach Age Verification?. *The Center for Growth and Opportunity*. https://www.thecgo.org/research/keeping-kids-safe-online-how-should-policymakers-approach-age-verification/.

British Standards Institution. (31.03.2018). *PAS 1296:2018 Online age checking. Provision and use of online age check services. Code of Practice*.

Commission for the Protection of Minors in the Media. (12.05.2022). *Kriterien zur Bewertung von Konzepten für Altersverifikationssysteme als Elemente zur Sicherstellung geschlossener Benutzergruppen in Telemedien nach § 4 Abs. 2 S. 2 JMStV*. https://www.kjm-online.de/fileadmin/user_upload/KJM/Themen/Technischer_Jugendmedienschutz/AVS-Raster_gueltig_seit_12.05.2022-ENG.pdf.

Committee for Standardization and European Committee for Electrotechnical Standardization. (Sep 2023). *Age appropriate digital services framework*. https://www.cencenelec.eu/media/CEN-CENELEC/CWAs/ICT/cwa18016_2023.pdf.

Committee on the Rights of the Child. (02.03.2021). *General comment No. 25 (2021) on children's rights in relation to the digital environment*. CRC/C/GC/25. https://digitallibrary.un.org/record/3906061?ln=en.

Communications Regulatory Authority. (06.03.2024). *CONSULTAZIONE PUBBLICA DI CUI AL COMMA 4 DELLA DELIBERA N. 9/24/CONS PER L'APPROVAZIONE DI UN PROVVEDIMENTO CHE DISCIPLINA LE MODALITÀ TECNICHE E DI PROCESSO PER L'ACCERTAMENTO DELLA MAGGIORE ETÀ DEGLI UTENTI AI SENSI DELLA LEGGE 13 NOVEMBRE 2023, N. 159*. https://www.agcom.it/documents/10179/33556820/Allegato+25-3-2024+1711363896057/490138bb-c739-4f2f-81ac-21acc717767e?version=1.0.

Data Protection Commissioner. (Dec 2021). *Fundamentals for a Child-Oriented Approach to Data Processing*. https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf.

Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services, OJ L 151, 7.6.2019, p. 70–115.

eSafety Commissioner, Australia. (Aug 2023). *Roadmap for age verification and complementary measures to prevent and mitigate harms to children from online pornography*. https://www.esafety.gov.au/sites/default/files/2023-08/Age-verification-background-report.pdf.

euCONSENT, (n.d.). *EUCONSENT. ELECTRONIC IDENTIFICATION AND TRUST SERVICES FOR CHILDREN IN EUROPE. Creating a safer digital world for children throughout the European Union*. https://euCONSENT.eu/.

euCONSENT. (29.06.2021). *D5.1 Common Vocabulary*. https://euCONSENT.eu/project-deliverables/.

euCONSENT. (Sept 2021). *EU Member State Legal Framework*. https://euCONSENT.eu/project-deliverables/.

euCONSENT. (02.01.2022). *D2.2 EU Methods for AVMSD and GDPR Compliance Report*. https://euCONSENT.eu/project-deliverables/.

European Commission. (n.d.). *A digital ID and personal digital wallet for EU citizens, residents and businesses*. https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/EU+Digital+Identity+Wallet+Home.

European Commission. (11.05.2022). *A Digital Decade for children and youth: the new European strategy for a better internet for kids (BIK+)*. https://digital-strategy.ec.europa.eu/en/library/digital-decade-children-and-youth-new-european-strategy-better-internet-kids-bik.

European Commission. (11.05.2022). *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS. A Digital Decade for children and youth: the new European strategy for a better internet for kids (BIK+)*. COM(2022) 212 final. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022DC0212.

European Commission. (30.01.2024). *Digital Services Act: Task Force on Age Verification*. https://digital-strategy.ec.europa.eu/en/news/digital-services-act-task-force-age-verification-0.

European Commission. (20.03.2024). *Second Meeting of the Task Force on Age Verification*. https://digital-strategy.ec.europa.eu/en/news/second-meeting-task-force-age-verification.

European Data Protection Supervisor. (n.d.). *Necessity & Proportionality*. https://edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality_en.

European Telecommunications Standards Institute. (Mar 2021). *Accessibility requirements for ICT products and services*. EN 301 549. https://www.etsi.org/deliver/etsi_en/301500_301599/301549/03.02.01_60/en_301549v030201p.pdf.

Government Communications Headquarters UK. (Nov 2020). *VoCO (Verification of Children Online). Phase 2 Report*. https://www.gov.uk/government/publications/voco-verification-of-children-online-phase-2-report.

Information Commissioner's Office. (15.01.2024). *Information Commissioner's opinion: Age Assurance for the Children's Code*. https://ico.org.uk/about-the-ico/what-we-do/information-commissioners-opinions/age-assurance-for-the-children-s-code/.

Information Commissioner's Office. (n.d.). *'Likely to be accessed' by children – FAQs, list of factors and case studies.* https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/likely-to-be-accessed-by-children/#threshold.

Institute of Electrical and Electronics Engineers. (Feb 2024). IEEE Approved Draft Standard for Online Age Verification. *IEEE P2089.1/D2.1*.

International Organization for Standardization. (n.d.). *ISO/IEC WD 27566. Information security, cybersecurity and privacy protection. Age assurance systems Framework*. https://www.iso.org/standard/80399.html.

International Organization for Standardization. (n.d.). *ISO/IEC WD 27566-1. Information security, cybersecurity and privacy protection. Age assurance systems Framework. Part 1: Framework*. https://www.iso.org/standard/88143.html.

International Organization for Standardization. (n.d.). *ISO/IEC WD 27566-2: Age assurance systems. Part 2: Benchmarks for benchmarking analysis*. https://www.iso.org/standard/88147.html.

International Organization for Standardization. (Nov 2021). *ISO Working Draft Age Assurance Systems Standard*. https://euCONSENT.eu/download/iso-working-draft-age-assurance-systems-standard/.

Leiden University & Considerati. (Mar 2023). Children's Rights Impact Assessment. *Ministry of the Interior and Kingdom Relations, Netherlands*. https://www.nldigitalgovernment.nl/overview/childrens-rights-online/dossier-documenten/childrens-rights-impact-assessment-manual/.

Livingstone, S., & Stoilova, M. (2021). The 4Cs: Classifying online risk to children. *Leibniz-Institut Für Medienforschung | Hans-Bredow-Institut (HBI)*. https://doi.org/10.21241/ssoar.71817.

Media Commission. (08.12.2023). *Consultation Document: Online Safety*. https://www.cnam.ie/wp-content/uploads/2023/12/Draft_Online_Safety_Code_Consultation_Document_Final.pdf.

Milkaite, I., & Lievens, E. (2020). Child-friendly transparency of data processing in the EU: from legal requirements to platform policies. *Journal of Children and Media*, *14*(1), 5-21.

National Markets and Competition Commission. (n.d.). *PUBLIC CONSULTATION ON THE CRITERIA FOR ENSURING THE APPROPRIATENESS OF AGE VERIFICATION SYSTEMS ON VIDEO-SHARING PLATFORM SERVICES FOR CONTENT THAT IS HARMFUL FOR MINORS*. INF/DTSA/329/23. https://www.cnmc.es/sites/default/files/editor_contenidos/Audiovisual/1_1_INF_DTSA_329_23_Public%20consultation%20age%20verification%20CNMC%20Spain_eng.pdf.

National Institute of Standards and Technology. (n.d.). *Face Analysis Technology Evaluation (FATE) Age Estimation & Verification*. https://pages.nist.gov/frvt/html/frvt_age_estimation.html.

Office of Communications. (05.12.2023). *Guidance on age assurance and other Part 5 duties for service providers publishing pornographic content on online services*.

https://www.ofcom.org.uk/__data/assets/pdf_file/0018/272601/guidance-part-5-annexe-2.pdf.

Organization for Economic Cooperation and Development. (2021). *Children in the digital environment: Revised typology of risks*. https://www.oecd-ilibrary.org/science-and-technology/children-in-the-digital-environment_9b8f222e-en.

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, COM(2022) 454 final, (15.09.2022).

Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework. OJ L 2024/1183, 30.4.2024.

Regulatory Authority for Audiovisual and Digital Communication. (April 2024). *Consultation publique sur le projet de référentiel déterminant les exigences techniques minimales applicables aux systèmes de vérification de l'âge mis en place pour l'accès à certains services de communication au public en ligne et aux plateformes de partage de vidéos qui mettent à disposition du public des contenus pornographiques*. https://www.arcom.fr/sites/default/files/2024-04/Arcom-Consultation-publique-projet-referentiel-determinant-exigences-techniques-minimales-applicables-aux-systemes-verification-age-acces-contenus-pornographiques-en-ligne.pdf.

Sas, M., & Mühlberg, J. T. (2024, February). Trustworthy Age Assurance?. In *The Greens Cluster: Social & Economy, Location: The European Parliament*. https://www.greens-efa.eu/en/article/document/trustworthy-age-assurance.

Shaffique, M.R. & van der Hof, S. (Feb 2024). Research report: Mapping age assurance typologies and requirements. *European Commission*. https://data.europa.eu/doi/10.2759/455338.

Spanish Data Protection Agency. (Dec 2023). *Decálogo de principios. Verificación de edad y protección de personas menores de edad ante contenidos*

*inadecuados.*https://www.aepd.es/guias/decalogo-principios-verificacion-edad-proteccion-menores.pdf.

United Nations Children's Fund. (Apr 2021). *Digital Age Assurance Tools and Children's Rights Online across the Globe: A Discussion Paper*. https://c-fam.org/wp-content/uploads/Digital-Age-Assurance-Tools-and-Childrens-Rights-Online-across-the-Globe.pdf.

www.betterinternetforkids.eu

@Insafenetwork
@safeinternetday

facebook.com/saferinternet
facebook.com/SaferInternetDay

linkedin.com/company/better-internet-for-kids

youtube.com/@insafe01

info@betterinternetforkids.eu

Better Internet for Kids